A “Trusted Information Network” for the National Responder Community

Karen Donahue

Director, Homeland Security Programs

Tel: 202-312-5907
kdonahue@lucent.com

Bob Cooil

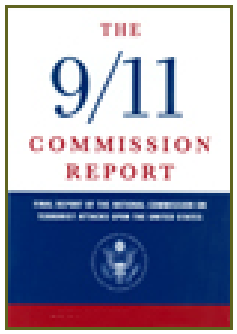
Director, Government Technical Support

Tel: 336-279-7031
cooil@lucent.com

Lucent Technologies
Bell Labs Innovations

The Challenge

- **To provide "National Responder" stakeholders the means to communicate and share mission-critical data between each other.**
- **To provide "National Responders" field-access to "Trusted Information Networks".**
- **The 9/11 Commission Report cited:**
  - "The inability to communicate was a critical element at the World Trade Center, the Pentagon, and Somerset County, Pennsylvania crash sites, where multiple agencies and multiple jurisdictions responded. The occurrence of this problem at three very different sites is strong evidence that compatible and adequate communications among public safety organizations at the local, state,and federal levels remains an important problem." (p397)



  - *"Congress should support pending legislation which provides for the **expedited and increased assignment of radio spectrum** for public safety purposes."* (p397)
  - ***"The President should…** coordinate the resolution of the legal, policy, and technical issues across agencies to **create a "trusted information network."*** (p418)

Vision for "Trusted Information Network"

- **Serves ALL public safety users – the National Responder community. Estimated to be in the 8 -10M user range.**
  - Joint use of broadband spectrum allocation by NTIA and FCC Responder Communities
- **National availability and interoperability – Not just regionally or within a particular urban area.**
  - National broadband network would become the "universal transport layer" for this community,
- **Secure, interoperable, broadband capability and redundant voice (VOIP).**
  - VOIP can supplement existing public safety voice capabilities.
  - Network accessed from commercial or customized handheld or vehicle-mounted devices.
  - Can send real-time video, high-resolution images, and geo-spatial data
- **Commercial standards would provide significant cost savings to the U.S. taxpayer.**
  - Large numbers of commercial vendors able to enter the marketplace and develop mission-specific hardware / software applications.
  - Nation-wide capability can be implemented within 24 months.
- **Could provide Rural Broadband Interconnectivity in some geographic areas.**
  - Portions of the spectrum *could* be used on secondary or flexible basis for other services (example: rural broadband) that many seek.
  - Doing so should not impact Nat'l Responder capacity, and could provide source of additional funding for network infrastructure in less populated areas.

The “National Responder” Community:

- **8-10M Million Users**
  - 2.5M First Responders (Police, Fire, EMT)
  - National Response and Federal Response Plan users
  - National Incident Management System (NIMS) users
  - National Security /Emergency Preparedness (NS/EP) users
  - Federal Agencies with Public Safety, Investigation and Asset Protection Missions
    - Example: FEMA, Transportation, Customs/Border Control
  - Critical Infrastructure owners, operators, decision makers
  - Key municipal leadership and decision makers
  - Military Support (ex. NorthCom, National Guard)
  - Public health system (Hospitals, CDC, etc.)

Why a National Responder Broadband Network?

- **National Response workers have no common spectrum operational platform – Two separate spectrum regulators:**
  - **FCC: Public Safety, Utilities**
    - FCC has allocated 50 MHz at 4.9 GHZ for broadband data applications
    - No other National Responders can use this allocation
  - **NTIA: Federal Agencies, DoD**
    - There is NO broadband spectrum allocated for Federal Public Safety entities
- **National Response field workers have virtually no mobile access to data**
  - Current data applications in the 19.2 kbps range
  - In contrast, 78% of US Enterprises have access to Broadband capabilities
- **Significant government information sharing initiatives will remain isolated if there is no secure way to get that information to the field.**
  - Ex. Chimera, Global Information Grid, Information Sharing /Analysis Center
- **Creating a dedicated, secure, broadband mobile network will:**
  - **Place this constituency on par with commercial enterprises, and**
  - **Provide fulcrum to create enhanced capabilities and applications**

SEC. 7502. STUDIES ON TELECOMMUNICATIONS CAPABILITIES AND REQUIREMENTS

(a) ALLOCATIONS OF SPECTRUM FOR EMERGENCY RESPONSE PROVIDERS.—The Federal Communications Commission shall, in consultation with the Secretary of Homeland Security and the National Telecommunications and Information Administration, conduct a study to assess short-term and long-term needs for allocations of additional portions of the electromagnetic spectrum for Federal, State, and local emergency response providers, including whether or not an additional allocation of spectrum in the 700 megahertz band should be granted by Congress to such emergency response providers.

(b) STRATEGIES TO MEET PUBLIC SAFETY TELECOMMUNICATIONS REQUIREMENTS.—The Secretary of Homeland Security shall, in consultation with the Federal Communications Commission and the National Telecommunications and Information Administration, conduct a study to assess strategies that may be used to meet public safety telecommunications needs, including—

(1) the need and efficacy of deploying nation- wide interoperable communications networks (including the potential technical and operational standards and protocols for nationwide interoperable broadband mobile communications networks that may be used by Federal, State, regional, and local governmental and nongovernmental public safety, homeland security, and other emergency response personnel);
(2) the capacity of public safety entities to utilize wireless broadband applications; and
(3) the communications capabilities of all emergency response providers, including hospitals and health care workers, and current efforts to promote communications coordination and training among emergency response providers.

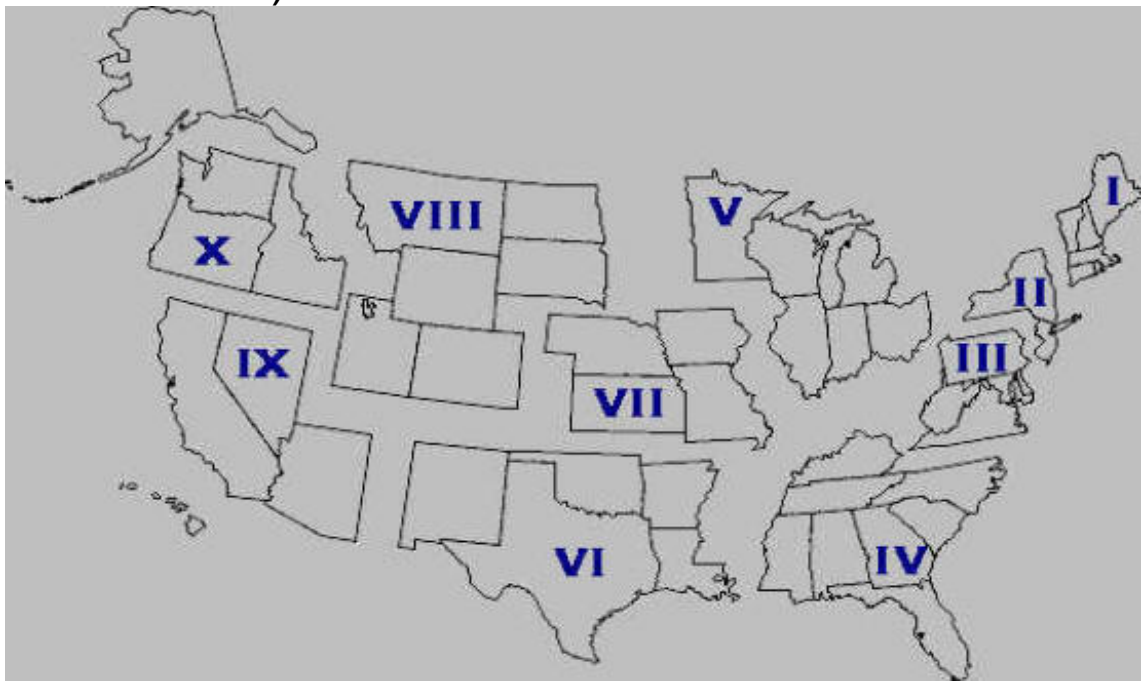
(c) STUDY REQUIREMENTS —In conducting the studies required by subsections (a) and (b), the Secretary of Homeland Security and the Federal Communications Commission shall—

(1) seek input from Federal, State, local, and regional emergency response providers regarding the operation and administration of a potential nation-wide interoperable broadband mobile communications network; and
(2) consider the use of commercial wireless technologies to the greatest extent practicable.

A National Responder Network: *One Model*

National Oversight: Regional Implementation

- "P/S Carriers" Bid for / Lease Spectrum for each Region
- "P/S Carriers" Build, Operate and Maintain Networks per specifications
- "P/S Carriers" can use spectrum/network for secondary basis
  (ex. Rural Broadband)



- Agencies Pay for Devices and Services
- Agencies Develop Applications Unique to their Mission
- Agencies Create Policy for Access to their Data

Benefits of Public/Private National Network

- ✓ Potential National Responder (NR) community increased in size sufficient to warrant special-purpose classification/treatment
- ✓ Commercial service + dedicated spectrum build-out will provide the QoS that the NR community requires *without undermining commercial market position*
  - Leverages carrier-grade, commercial assets to provide superior capabilities to this community.
  - Creates attractive market for private sector investment, thus relieving U.S. taxpayer of multi-billion dollar outlays.
  - Utilize commercial technologies (IP-orientation)
- ✓ Special-purpose spectrum could meet two public interest objectives
  - Public safety/Homeland security
  - Rural Broadband (on secondary basis) to address the est. 20M subscribers not currently served

Concept in Operation: ARJIS

Automated Regional Justice Information System (San Diego)

ARJIS is a complex criminal justice enterprise network utilized by 50 local, state and federal agencies in the San Diego region. Supports a regional, web-based enterprise network that utilizes technical and operational standards to build interfaces to all criminal justice systems in the region.

ARJISNet secure intranet contains data on the region's crime cases, arrests, citations, field interviews, traffic accidents,fraudulent documents, photographs, gang information and stolen property.

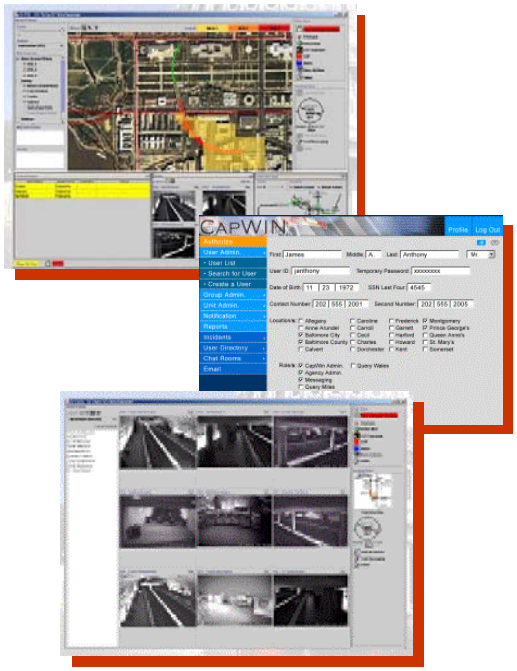
ARJISNet integrates over 2,500 workstations and printers throughout the 4,265 square miles of San Diego County.

Over 10,000 registered and authorized users generating over 35,000 transactions daily (1000 with mobile access). ARJIS is also utilized for tactical analysis, investigations, statistical information and crime analysis. Officers and investigators can additionally request electronic notification when information is obtained by another agency or officer concerning an individual, location or vehicle. The critical success factor for ARJIS is the "single point of entry" to query all regional justice data.

Mobile Access to this Network is provided through a commercial service provider (Verizon Wireless) and uses commercial, standards-based technology (CDMA EV-DO)

Commercial 3G Technologies: Benefits Today

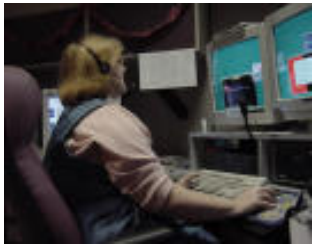
- **Enable first responders to use critical applications they already have not accessible on slower speed networks**
  - Mapping/Location Based Services – critical infrastructure protection
  - Video Streaming – incident scenes, security
  - Digital Image transfer – disaster scene
  - Large files transfer- records, on-line manuals, emergency protocols
  - Biometrics – facial recognition
  - Bio-terrorism detection and response – sample analysis, plume tracking



- **Field Access to the Trusted Information Network**
  - Secure and authorized access to critical data
  - Sufficient capacity for emergencies

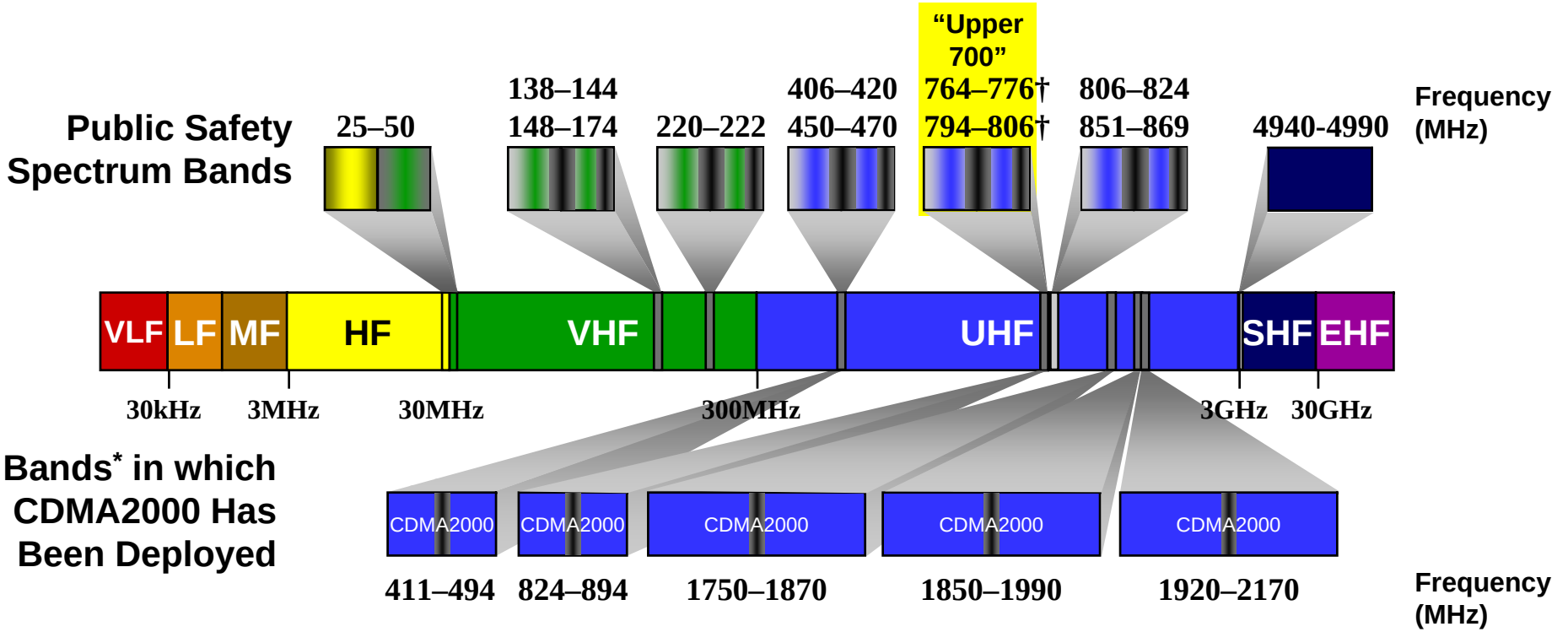
One *Potential* Commercial Technology: cdma2000 EVDO

- Commercially proven
- Deployed at national scale by major commercial carriers
  - More than 20 vendors of infrastructure and services
  - More than 48 terminal vendors with more the 486 devices



- Data rates of at least 156.0 kbps /sec uplink and 2 Meg/sec downlink
  - Increases to 1.5 MB/3MB in 2006
  - VOIP support in 2006
- Security / Encryption fully incorporated at all levels
- Functional Interoperability
  - Full interoperability with systems employing IP and PSTN interfaces
  - Ubiquitous use of IP and PSTN interfaces in public safety and all levels of government

3rd Generation Technologies: Successfully Deployed in a Variety of Spectral Bands



* 13 band classes defined for CDMA2000

†Currently occupied by TV channels

Band-shifting 3G technologies allows US to leverage 3G features and economies of scale

Summary

- Nation-wide broadband +VOIP capability could be achieved quickly and cost-effectively by leveraging commercial technologies ***plus*** dedicated spectrum for assured access.

- By aggregating this community, a new user class is created that the private sector would compete to service, thus lowering infrastructure and O & M costs for the government at federal, state and local levels.

- The resulting “universal transport layer” could be leveraged for a multitude of advanced homeland security applications, including sensor networks, bio-metric systems and surveillance capabilities – all at far lower costs than currently envisioned.

- Could also be utilized to deliver rural broadband services to the 20M potential subscribers not currently served.